MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2019/2020

TDF3241 – DIGITAL FORENSICS

(All Sections / Groups)

7 MARCH 2020
9:00 AM – 11:00 AM
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 4 pages (including cover page) with 5 Questions only.

2. Attempt **ALL** questions. The distribution of the marks for each question is given. This paper carries **50 marks**.

3. Please print all your answers in the Answer Booklet provided.

Question 1 (10 Marks)

(a) You are called to investigate a computer for a court case. Point out FOUR (4) main stages in the process of doing this from the notification of requiring your services to the final verdict of the court case. [4 marks]

(b) As a lab manager in a digital forensics secure facility, you are required to produce FOUR (4) recommendations for securing storage containers to contain the evidence in a secure facility where the digital forensics investigation is conducted. [4 marks]

(c) Point out TWO (2) ways you can minimize the risk of static electricity which may damage or corrupt the evidence media stored in your secure facility. [2 marks]

[TOTAL = 4 + 4 + 2 = 10]

Question 2 (10 Marks)

(a) Distinguish THREE (3) advantages and TWO (2) disadvantages of choosing the raw image file format for data acquisition in a digital forensics investigation. [5 marks]

(b) In order to analyse a seized hard disk from a crime scene, you have to distinguish FIVE (5) components of a hard disk drive. [5 marks]

[TOTAL = 5 + 5 = 10]

Continued ...

Question 3 (10 Marks)

(a) You have a disk image which contains the following hex sequence.

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F 10 11 12 13 14 15 0123456789ABCDEF012345
00000000 FF D8 FF E0 20 66 66 65 30 20 30 30 31 30 20 34 61 34 36 20 34 39 .... ffe0 0010 4a46 49
00000016 34 36 20 30 30 30 31 20 30 31 30 31 20 30 30 36 30 20 20 2E 2E 2E 46 0001 0101 0060  ...
0000002C 2E 2E 2E 4A 46 49 46 2E 2E 2E 2E 2E 60 0A 30 30 37 39 37 63 31 30 ...JFIF.....`.00797c10
00000042 3A 20 30 30 36 30 20 30 30 30 30 20 66 66 64 62 20 30 30 34 33 20 : 0060 0000 ffdb 0043
00000058 30 20 20 01 00 20 27 20 27 20 20 20 22 20 20 24 20 01 20 27 7F 000a 0101 0007 05fa
```

Analyse the above sequence and discover what kind of file is stored on this disk image. Demonstrate TWO (2) ways you can know this in order to justify your answer. [5 marks]

(b) Scope creep often happens in forensics investigation that can be time consuming. Define scope creep in digital forensics. [1 mark]

(c) Bit-shifting is a well-known technique for hiding data from unauthorized access by others. Explain how this technique works. [2 Marks]

(d) AccessData software has a separate database, the Known File Filter (KFF) to discriminate the data using hash values. Explain how KFF works. [2 Marks]

[TOTAL = 5 + 1 + 2 + 2 = 10]

Continued ...

Question 4 (10 Marks)

(a) Graphics are stored in one of the three types of graphics files: bitmap, vector and metafile. Show the difference between them. [3 Marks]

(b) You are trying to open a graphics file in an image viewer but you can't see its content. What you are going to do to fix this problem? [2 Marks]

(c) What are the TWO (2) major techniques of steganography to hide data in an image file? Explain each of them. [4 Marks]

(d) Explain the terms of Order of Volatility (OOV). [1 Mark]

[TOTAL = 3 + 2 + 4 + 1 = 10]

Question 5 (10 Marks)

(a) You as a network security analyst in a company encountered abnormal activities on the server. You suspect that the network has been attacked by an unauthorized person. What actions you could take in order to gather the evidence? [2 Marks]

(b) The main concerns with mobile devices are loss of power and synchronization with PCs. Therefore, proper search and seizure procedures are critical. Provide FOUR (4) acquisition procedures for the mobile devices. [4 Marks]

(c) Assume that you are computer forensics examiner. Sometimes, you are required to prepare an examination plan for the attorney. What is an examination plan and how does it help in your testimony? [4 Marks]

[TOTAL = 2 + 4 + 4 = 10]

END OF EXAM PAPER